CTSC

CENTER FOR TRUSTWORTHY
SCIENTIFIC CYBERINFRASTRUCTURE

The NSF Cybersecurity Center of Excellence

Developing Cybersecurity Programs for NSF Projects and Facilities

Bob Cowles, Craig Jackson, Jim Marsteller

2017 NSF Cybersecurity Summit
August 15, 2017

http://hdl.handle.net/2022/21725

Wireless Access Point:

WestinConference

Access Code:

nsf0816

CTSC

Outline

1. Introduction
2. What is a cybersecurity program?
3. Founding a program
4. Maintaining a program
5. Evaluating and optimizing a program

Introductions:

Name, Org, Why here?

1. Introduction

Evolution of this training and the Guide

History

1. August 2014: Guide published (trustedci.org/guide)
2. August 2014: First time doing a version of this training
3. April 2015: LFM Subsection Draft first delivered
4. August 2017: LFM Subsection Draft most recently delivered
5. September 2017: Beginning major revision to Guide
6. *…. We've learned a lot from our 25+ engagements, appearances, community survey, being here with you.*

Meanwhile

7. Cyber problem is not getting easier for anyone
8. Proliferation of cybersecurity frameworks, regulations, "solutions"
9. NSF science cannot afford to remain scattered and immature
10. NSF science cannot afford wasteful efforts

Thus

11. Changes to the training and Guide: Increasing focus on fundamentals and how to get started, but retain tailoring to the NSF science community's mission, needs, and capabilities. Increasing specificity about do's and don't's.

Goals of this training:

1. Introduce NSF LFs, CI projects, support organizations, and NSF POs to the cybersecurity program concept.
2. Provide actionable guidance, resources, and tools that help you get started or get serious.
3. Add perspective on special issues and challenges.
4. Answer your questions. Hear your concerns.

How this happened

How is our stuff different?

1. Tailored to and informed by the NSF community
2. Focused on *both* effectiveness and efficiency
3. Publicly available and free to use (unlike, *e.g.*, ISO)
4. Templates, templates, templates!!!

Note:

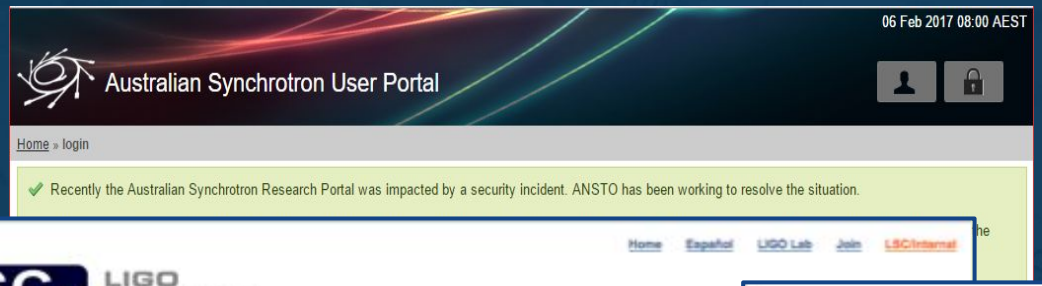
- We'll make frequent mention of the Guide and its resources at trustedci.org/guide.
- We want and need to know if you are or end up using our guidance.

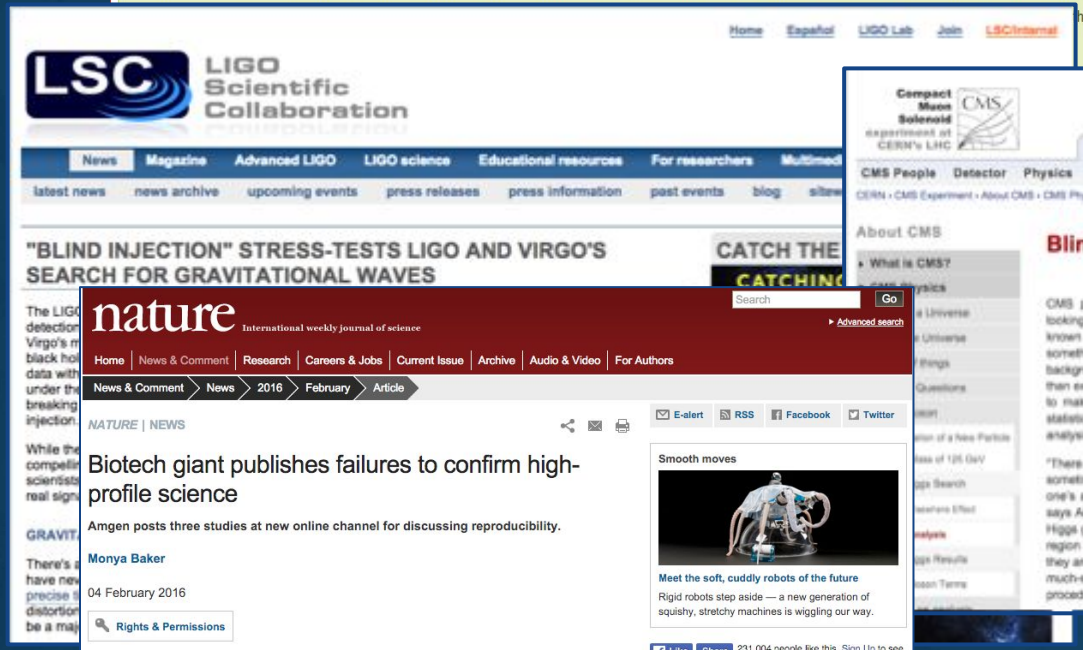
Ground Rules

1. Interrupt us. Ask questions. Offer opinions.
   a. We will probably interrupt each other.
   b. We do have a number of designated times for Q&A.
2. If we throw out a term that you don't understand, please stop us!
3. We use "information security" and "cybersecurity" more or less interchangeably. We often prefer the former, but have gotten trapped in the cybereverything.
4. Slides are or will be available. trustedci.org/survey
5. It may feel like it, but we're not going to cover everything… e.g., if you're developing and distro'ing software, you have an additional set of sec practices to address.
6. Break at 4pm.
7. Please complete the training eval survey.
8. Please be sure you sign in.

Why does cybersecurity matter for science?

Science must be trustworthy and reproducible





CTSC

“I’m doing open science… I don’t need cybersecurity.”

1. Information has always been central to science.
2. And, the Internet’s severe weather conditions impact everyone who is connected.
3. Cybersecurity is about confidentiality, availability, and integrity of information and information systems.
   a. Availability of instruments and systems.
   b. Trust in and availability of the data.
4. Reputation, trust, and other “intangibles” matter.
5. Imposition of inappropriate/inefficient/ineffective compliance regimes can be a real distraction.

Balance is Key:
Risk versus Mission

Minimize:

Cost of breaches/incidents

+

Cost of cybersecurity program

+

Impact on science productivity

Text paraphrased from: "The Defender's Dilemma. Charting a Course Toward Cybersecurity"
http://www.rand.org/pubs/research_reports/RR1024.html

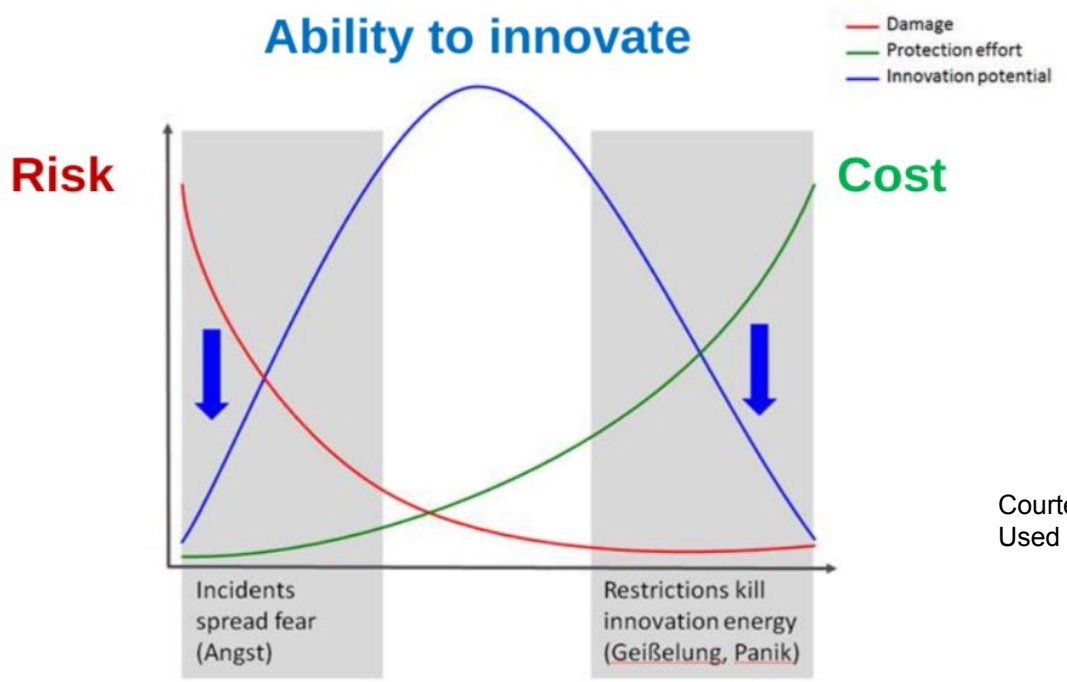
CTSC

Provide Guardrails, not Barriers

SIEMENS

Economic Trade-off:
Relationship between risk, cost and ability to innovate

Too little and too strong security governance are hindering innovation



Courtesy of Rolf Reinema
Used with Permission

CTSC

2.
What is a cybersecurity program?

It’s not a “plan”; it’s not a single project.

A cybersecurity program is a structured approach to develop, implement, and maintain an environment conducive to appropriate levels of information security and risk to the organization’s mission [i.e., your science mission].

Cybersecurity programs are made up of ongoing activities and projects in the areas of: policies and procedures; controls and mitigations; control verification and assessment; threat monitoring and activity analysis; incident response and remediation; and training and awareness.

Cybersecurity programs should be scoped to the key assets, resources, and lifespan of organizations.

Bottom line:

Security programs are living, breathing things.

CTSC

Why approach this *programmatically*?

Cybersecurity...

1. Is complex and multidisciplinary
2. Takes time and resources to address competently
3. Is always relevant, regardless of where you are in your project's life

Seemingly intractable problems become workable when we chop them up in time and space. Projects and ongoing activities. Prioritize.

Pillars of a Cybersecurity Program

1. Governance

   Roles, Processes, Policies, Requirements

2. Resources

   People, Infrastructure, and Security Tools…
   Money

3. Controls

   Procedural, technical, administrative safeguards and countermeasures

Q&A

Who here is at the “building a program” stage?
Who’s at the “improving my program” stage?

3.
Founding a program

Section 3 Outline

Critical Caveat: Project Phase, Size, and Complexity

3.a. Resources

First Steps

Special Topics: Shelfware

3.b. Governance

First Steps

Special Topics: Policy Development, Project Management, Risk Management Frameworks

3.c. Controls

First Steps

Special Topics: Identifying Information Assets, Risk Assessments

3.d. Addressing Project Phase

Critical Caveat:

Project Phase, Size, and Complexity

Project Phase, Size, Complexity

Phase matters: *pretty different scenarios….*

- A newly funded project that doesn't go operational for several years
- An operational facility that's been around for several years that is finally waking up to the need for a cybersecurity

Other variables:

1. Overall budget
2. IT budget
3. Cybersecurity budget?
4. # of personnel
5. Geographic and institutional distribution
6. Role and importance of information assets
7. Institutional support

Project Phase, Size, Complexity

Our working assumptions:

1. You have some freedom or need to define a program for your project and facility. No one is going to do it all for you.
2. You are not so resource constrained that some cybersecurity basics are impossible.

But, at the end of Sec 3, we'll talk about strategies for dealing with some of the variables.

3.a. Resources

Resources:
First Steps

1. Develop a budget
   a. Decide what is in/out of the budget (staff, tools, training)
   b. What are good IT practices vs. cybersecurity?
2. Invest in people
   a. A variety of specific skills are required
   b. Need frequent training and contact with peers

Resources: Budget

- Security costs money.
  - Hint: Joining forces and sharing practices and information leads to economy of scale.
- Cybersecurity budgets lie between 3% to 12% of IT budgets. (Smaller is higher)*
- Variance on what is included in cybersecurity budget
- Distinguish between good practices (business and IT) and actual cost of cybersecurity

* See: 2016 NSF Cybersecurity Summit Report for details: http://hdl.handle.net/2022/21161

Resources: People

Invest in people!

1. Hire *security practitioners*, and support their professional development.
   a. Consider: CTSC Training (more later), Information Security Practice Principles (cacr.iu.edu/principles)
2. Collaborate across silos.
3. Build partnerships, leverage collective action, look to similar entities doing things well.

Resources: People

- Technical skills around networks, operating systems and applications, security tools
- Teaching skills to educate users on cybersecurity
- Communication skills to put cybersecurity risks into terms relating to the scientific mission
- Negotiating skills to arrive at acceptable risk mitigations

- Unlikely to find these skills in a single person, particularly without professional development

Special Topic: Shelfware

Beware of Shiny Objects

Examples:

Sophisticated log collection and analysis software

Fancy firewalls with advanced capabilities

IDS/IPS software that generates alerts upon seeing "suspicious activity"

Staff and training resources required are significant

Q&A

Blink twice if you feel very budget constrained.

CTSC

3.b. Governance

Governance:
First Steps

1. Determine whether and how relationships and requirements will help or burden you. (How does the outside world impact you?)
2. Develop core policy with special attention to roles and responsibilities, and risk acceptance. (Shape the inside world.)

Governance: Relationships…

… play a key role in a cybersecurity program

Cyberinfrastructure(CI): Research environments that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the Internet beyond the scope of a single institution.

Project Relationships

You are not alone

CI Projects are becoming increasingly distributed.

Multi-institutional, international, interdisciplinary but highly interconnected. Virtual project teams are commonplace.

While this can create challenges, it also creates opportunity.

Challenges of CI projects

- Disparate policies and requirements among collaborators - establishing MOUs
- Cultural differences (open research environments vs. restrictive govt labs); information sharing, communications, different compliance reqs
- Larger attack surfaces: users, servers, network connections, inconsistency with administration and management
- Specials: ICS/SCADA, one of a kind research data
- More actors: hacktivists, governments, bad users

Opportunities in CI Projects
"I've got your back"

- Collective knowledge a of distributed team can be a resource of support. "Has anyone seen this unusual network traffic?"
- Improve detection ability and response times by sharing event information. "Mass scanning from IP address 201.234.178.62, suggest blocking"
- Ad-hoc support in times of need.

CTSC

Governance: Requirements

1. Historically, lots of freedom. E.g., LF cooperative agreement terms give a LOT of breathing room.
2. Other potential sources of requirements
   a. Large Facility Manual
   b. Statutes and regulations (e.g., state or federal privacy law)
   c. Institutional policy
   d. Miscellaneous officious bureaucrats? (Craig joke)
3. Going forward, we assume you have a lot of choice and/or ability to negotiate. We also assume you have the ability to assimilate special requirements.

NSF Cooperative Agreements Information Security Requirement

- Incorporated in NSF's Supplemental Financial and Administrative Terms and Conditions
- Purpose is to help ensure that NSF large facilities and FFRDCs have policies, procedures and practices to protect research and education activities in support of the award
- Terms or requirements like this are increasingly common at the proposal stage.

Articles in Supplement to CA-FATC LF and CA-FATC FFRDC:

"Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee's responsibility.

Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee as part of the awardee's IT security program, in place or planned, to protect research and education activities in support of the award."

Articles in Supplement to CA-FATC LF and CA-FATC FFRDC:

"The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training and notification procedures in the event of a cyber-security breach. The Summary shall include the awardee's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subrecipients, researchers and others who will have access to the systems employed in support of this award."

Articles in Supplement to CA-FATC LF and CA-FATC FFRDC:

"The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and coordination activities among NSF awardees."

“Roles and Responsibilities”

CTSC Resources:

- *Master Information Security Policy and Procedures (MISPP)*
- *Acceptable Use Policy (AUP)*

“Risk Assessment”

CTSC Resources:

- *Information Asset Inventory*
- *Risk Assessment Table*
- *Open Science Cyber Risk Profile*

“Technical, Administrative, Physical Safeguards”

CTSC Resources:

- *Access Control Policy*
- *Asset-Specific Access and Privilege Specification*
- *Password Policy*
- *Physical Security Policy*
- *Disaster Recovery Policy*
- *Incident Response Policy and Procedures*

“Awareness and Training”

CTSC Resources:

- *Information Security Training and Awareness Policy*
- *CTSC “Cyber Hygiene” Information Security Training Slide Deck*

“Notification Procedures”

CTSC Resources:

- *Incident Response Policy and Procedures*

“Evaluation Criteria”

CTSC Resources:

- *Master Information Security Policy and Procedures (MISPP)*

“Appropriate Security Measures for Subrecipients, Researchers and Others”

CTSC Resources:

- *Acceptable Use Policy (AUP)*

CTSC

GOVERNANCE: Sound, sane risk-based decision making

1. Residual risk is the risk left over after controls are applied. In cyber (as in most of life), it is never zero.
2. Residual risk acceptance is the heart and soul of risk management.
3. Who accepts residual risk?
4. Communication is critical.
5. Must read:

   AFCEA's The Economics of Cybersecurity

AFCEA's The Economics of Cybersecurity

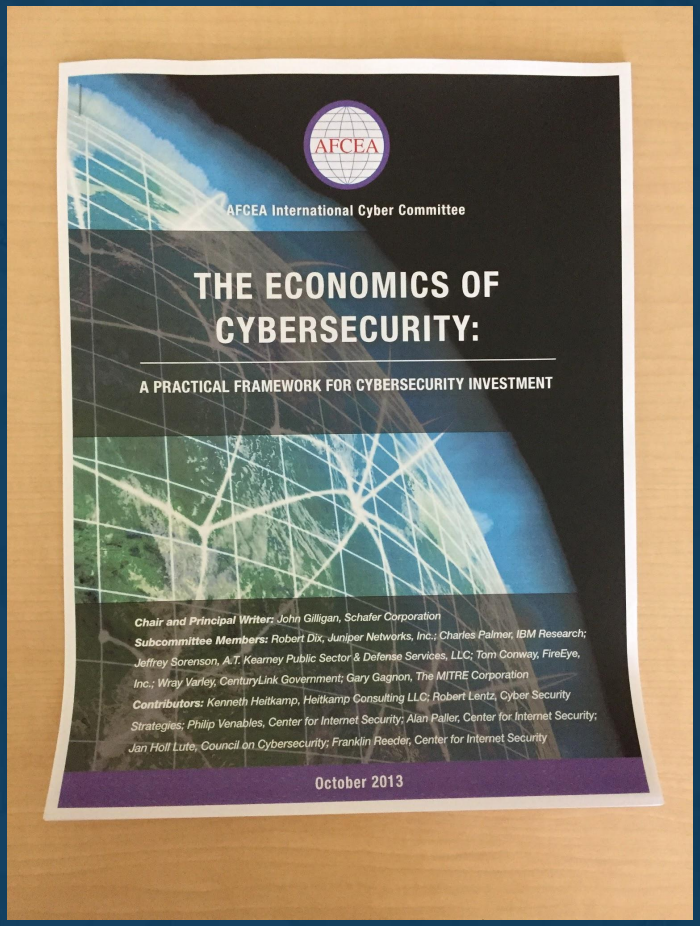
John Gilligan, fmr USAF CIO, now CIS

Background

1. Cyber has limited data for quantitative assessments.
2. Most cyber-attacks are unsophisticated.
3. Total protection is uneconomical.

Takeaways:

1. Focus on low-cost, high-impact interventions.
2. Prioritize defenses against common, unsophisticated attacks.
3. Utilize targeted defenses against high-sophistication, high-criticality attacks.
4. Accept risk of high-sophistication, low-criticality attacks.



CTSC

"If the highest aim of a captain were to preserve his ship, he would keep it in port forever."

- *Thomas Aquinas*

Governance: Roles and Responsibilities

Senior Management (e.g., PI, Director, CIO)

- Takes active role in allocating adequate resources, addresses program governance, accepts residual risk, and follows information security policies

Asset Owner

- Understands risks to the asset and ensures appropriate controls are in place while the assets are being developed, produced, maintained, and used

Chief Information Security Officer (CISO)

- Knowledgeable in information security, understands how information assets relate to the organization's mission, effectively communicates the issues and the tradeoffs; empowered as a decision-maker and key stakeholder where expert and timely action are required to protect organizational interests

Governance:
Importance of Project Leadership

PIs have the ultimate responsibility for ensuring the project has an effective information security program

- Promote the importance of a cybersecurity program
- Assigning security responsibilities
- Determine acceptable levels of risk
- Support cybersecurity program

Governance: Two Key Leadership Roles

Risk Acceptor: Weighs risks against project mission and accepts residual risk. Must have broad view of project. E.g. PI, technical lead. Must have ability to control the information assets and is responsible for the outcome of accepting those risks.

Cybersecurity Lead: Responsible for cybersecurity implementation & gauging residual risk. Must translate technical issues into management language. E.g. IT Security Professional, senior technical person.

Special Topic: Policy Development

Policy Development

You may not need a ton of written policy, but you need some.

Results in:

- Reproducible, communicable, and enforceable policy and processes.
- Artifacts that can be critiqued and evolved.

Craig's Policy Life Cycle:

(DAEFER?... Without "adopt" its just DEFER.)

1. *Develop*
2. *Adopt*
3. *Educate*
4. *Follow*
5. *Enforce*
6. *Revise*

The policy valley of death

CTSC

How much policy is enough?

CTSC

Policies we'll highlight

- Master Information Security Policy and Procedures (MISPP)
- Acceptable Use Policy (AUP)
- Incident Response Policies & Procedures
- Access Control Policy
- *A note about Privacy Policies*

(But… Physical security, disaster recovery, asset management, HR-specific, "specials" specific…. other policies can be critically important for your project.)

Templates!!!

We will refer to templates found at the following page: http://trustedci.org/guide

Cautionary Note: You will *have to* make these your own.

Master Information Security Policy & Procedures (MISPP)

Purpose: Core, general policies + guide for navigating the full corpus of policies and procedures.

Audience: You and all your stakeholders.

- Roles & Responsibilities (... CISO, Leadership)
- Developing, Implementing, and Maintaining Our Cybersecurity Program (... core processes)
- Resources & Key Contacts (... we're here to help)
- Other Policy and Procedure Documents (... a gateway of sorts)
- Enforcement provisions
- Terms & Acronyms
- *… plus anything else so central to the program that it warrants stating here*

Acceptable Use Policy (AUP)

Purpose: Establish a code-of-conduct for all users on the usage of a resource/information system.

Audience: You and all your stakeholders.

- Define rights and responsibilities of all users
- Establishes authority
- Consequences of infractions to policy (suspension, legal, criminal)
- Reduce Liability: disclaimers, no warranties
- Other Policy and Procedure Documents (Privacy, Password, management, Academic citation)
- Contact Information (General support, Emergency/Security)

Positive Statement	1. Purpose of [this system, organization, whatever]
General Good Behavior	2. Your use must be in alignment with [the purpose]
Specific Good Behavior	3. You must [responsibilities] a. Make a strong password
Bad Behavior	4. You must not do things contrary to [the purpose], including, but not limited to… a. Mining bitcoin b. … [nice to explain why, but don't have to]
Negative Consequences	5. Or else, you will be [nuked from orbit, scolded, cut off]

CTSC

Incident Response Policy

Purpose: Decide and document what to do in the event of a security incident BEFORE one happens, so that the response can be both rapid and well thought out.

Audience: IT and helpdesk staff, incident response team

- Define priorities for IR (e.g., relative importance of gathering forensic data vs. minimizing downtime)
- Who need to be notified, when, how, by whom; contact info
- Define who is responsible for which decisions
- Lay out response procedures for grey pigeon and black swan events
- IR team communication guidelines
- Specify when and how response procedures will be tested

Access Control Policy

Purpose: Define how access to various information assets (both systems and data) will be mediated, as well as who will be allowed access to what.

Audience: All users, stakeholders, and IT staff.

- You must first know what your assets are and need a data classification schema
- Least privilege principle
- Authentication vs. authorization
- Impacts every control

A note about privacy policies…

We didn't template one, on purpose.

- You may or may not be required to have one.
- You may or may not want to have one.
- Input is key…. think general counsel.
- Int'l collaboration can complicate things in a hurry.
- Want a template? Check out the BBB's.

Policy Development: Tips, Gotchas

- Do:
  a. Involve stakeholders (yes, even the relevant lawyers)
  b. Prioritize
  c. Use templates, examples
  d. Ask for help
  e. Share the resulting policies and train your personnel
- Please don't:
  a. Fall into the policy valley of death
     i. Allow policies to be developed and filed away without a formal approval process
     ii. Assume people will read them without education
     iii. Develop policies no one can or will enforce
  b. Work in a vacuum
  c. Assume you need one of each
  d. Be afraid to take this seriously
  e. Underestimate the power of v2

Special Topic: Project Management

Program and Project Management

1. Plans, goals, objectives, milestones, timelines, deliverables…. Your friends!
2. Enables prioritization. (A novel idea for many infosec people.)
3. Critical to turning seemingly intractable problems into workable issues.

* Shout out to Gemini Observatory and UNH Research Computing Center for sharing how project management enables security.

Special Topic: Risk Management Frameworks

Risk!

CTSC

Risk-based approaches?

- NIST Risk Management Framework*
- NIST Cybersecurity Framework, aka Framework for Improving Critical Infrastructure Cybersecurity
- HIPAA Security Rule*
- ISO 27005
- COBIT
- OCTAVE

* *blended or corrupted into compliance regimes*

Why risk management? Flexibility.

1. Compliance or rule-based approaches are generally inappropriate for infosec.
   a. *Dynamic hazard, relatively new, relatively low risk (for now)*
   b. *Security is not a solved problem*
   c. *Compliance is good when a solution has been proven to work.*
2. Allows for mitigation, transfer, avoidance, and acceptance of risk.
3. Well-suited for organizations with limited resources and time. Risk acceptance is on the table.
4. Still works if risk transfer is hard… if the type of risk is difficult to insure against or the "insured" is hard to identify.

Why avoid the existing risk management frameworks? Expense and inflexibility.

1. Risk management processes found in the existing frameworks (NIST RMF; NIST CSF) make questionable assumptions:
   a. Cybersecurity presents a measurable environment with some historical stability (e.g., actuarial history).
   b. Organizations have the time, money, and expertise to execute intensive procedural / documentation regimes.
2. As a result:
   a. Much time and money has been wasted on quasi-quantitative risk assessments with little or no validity…
      i. Rather than getting the basic processes and protections in place
   b. Frameworks like NIST RMF give lip service to risk management, but devolve into massive documentation games and checklist maintenance.

Alternative

1. Do the basic, healthy stuff with roles and risk we've already described.
2. AFCEA Economics of Cybersecurity

Q&A

3.c.
Controls

Controls:
First Steps

1. Select a reasonably scoped, prioritized, and evidence-based baseline control set.
2. Determine the relevance, feasibility, and current implementation state of these controls.

What to choose?

Many sets available, not all created equal:

NIST RMF, NIST CSF, ISO, HIPAA security rule,

CIS Critical Security Controls, ASD Essential Eight

More on NIST tomorrow.

Effective. Inclusive. Evidence-based. Adaptable.

Efficient. Doable. Affordable. Prioritized. Time-saving.

1. Choose reasonably scoped, prioritized, and evidence-based baseline control set.

CIS Critical Security Controls (aka the Top 20)

1. Prioritized!!! (*See, esp.*, Pescatore, Back to Basics: Focus on the First Six CIS Critical Security Controls)
2. Developed in a diverse, practitioner heavy environment. *E.g.*, NSA involved. (See, https://www.sans.org/critical-security-controls/history)
3. Updated frequently.
4. Testable and provable. (The plaintiffs bar and regulators will prefer this. So will technologists, engineers, and scientists.)
5. Good enough for Kamala Harris! (*See*, 2016 California Data Breach Report. The CSC's have the potential to become the de facto legal standard of "reasonable security" nationally.)

The First Six

CSC 1: Inventory of Authorized and Unauthorized Devices

CSC 2: Inventory of Authorized and Unauthorized Software

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

CSC 4: Continuous Vulnerability Assessment and Remediation

CSC 5: Controlled Use of Administrative Privileges

CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

1. Choose reasonably scoped, prioritized, and evidence-based baseline control set.

See also, ASD Essential Eight

1. Based on systematic study of actual attacks and breaches!!
2. Controls selected are those that would have prevented the most breaches
3. There are only 8!!! (or potentially 4)
4. Prioritized by how many breaches the control would have stopped
5. Clear implementation guidance

ASD Essential 8 / CIS CSC-6.1 Cross Walk

Application Whitelisting

CSC 2.2: Inventory of authorized and unauthorized software: Application Whitelisting

Disable untrusted MS Office Macros (may be less important for science)

CSC 2.2: Inventory of authorized and unauthorized software: Application Whitelisting

Patch Applications

CSC 3.1: Secure configurations for hardware and software: Refresh/update application versions
CSC 4.5: Continuous vulnerability assessment and remediation: Deploy automated patch management
CSC 18.1: Application software security: Install latest version and all relevant patches

User Application Hardening

CSC 3.1: Secure configurations for hardware and software: Install hardened version of applications
CSC 18.4: Application software security: Test applications for common security weaknesses

Restrict Admin Privileges

CSC 5.1: Controlled use of administrative privileges: Minimize administrative privileges

Multifactor Authentication

CSC 5.6: Controlled use of administrative privileges: Use multi-factor authentication for admin acces
CSC 16.11: Account monitoring and control: Require multi-factor for access to sensitive information

Patch Operating Systems

CSC 3.1: Secure configurations for hardware and software: Refresh/undate OS versions
CSC 4.5: Continuous vulnerability assessment and remediation: Deploy automated patch management

Daily Backup of Important Data

CSC 10.1: Data recovery capability: Frequent, automatic backup for systems with sensitive data

Orange = Original Top 4; Yellow = new additions

CTSC

Alan Paller, Director of Research, SANS Institute 8 Aug 2017

“NIST's willingness to say aloud that the old guidance [on password strength] was not correct is emblematic of a new approach we have been seeing at NIST. An equally impressive example of the shift to evidence-based guidance is their semi-public suggestions that the Australian "Essential Eight" or the Critical Security Controls "Top 5" (the two are nearly identical) are acceptable approaches to prioritizing actions that should be taken first in implementing the NIST Security Framework. Both the Essential Eight and the Top 5 are based on empirical evidence of what mitigations block and help mitigate damage from known attacks.”

2. Determine relevance, feasibility, and current implementation state

1. Relevance. The control set is a start, not an end. Some may be relevant only to certain data flows or systems.
2. Feasibility. There are amazing controls that may be effectively impossible.
3. Current factual state. What are you already doing? How do you know?
4. Example on next slide: Bob, JAM, and Craig work for a good size research project that operates out of a university. JAM is CIO. Craig is CISO. Bob just has to deal with us.

	A	B	C	D	E
1	Critical Security Control	Control Number	Control Description	Foundational?	Advanced
2					
3	**Inventory of Authorized and Unauthorized Devices**	**1**	**Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.**		
4		1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.	Yes	Use a mix of active and passive tools, and apply as part of a continuous monitoring program.

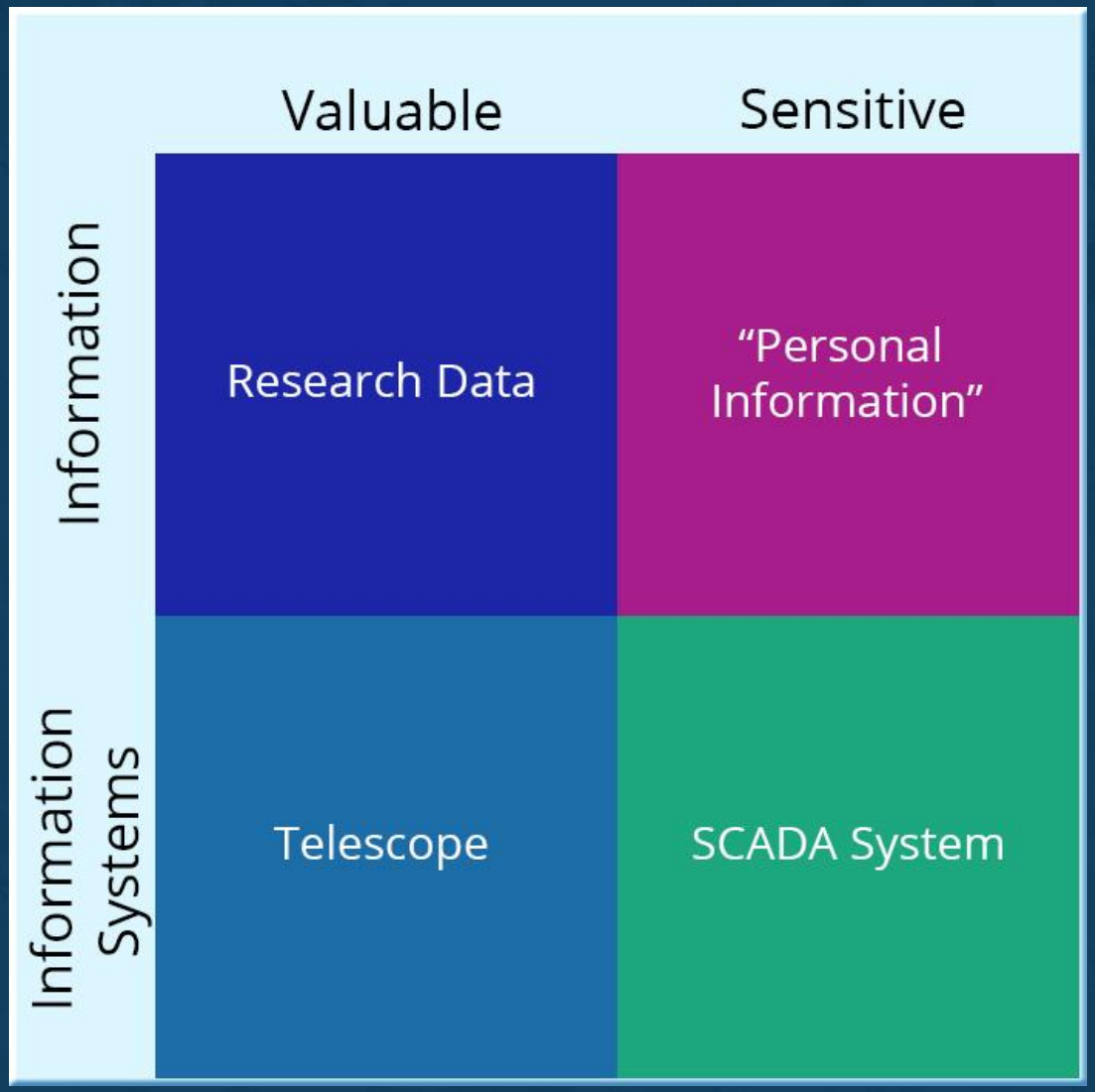
F	G	H	I
Relevant?	Status of Implementation	Assessment	Notes
Yes, No, Partial. Some ctrls are clearly relevant. Some may be clearly irrelevant to our environment. Some may be partially relevant. For "no" and "partial," include some prose as to why.	*Prose. Include enough detail that a decision maker can read the control description and the status and be able to make a judgment for the Assessment column, or at least be able to ask intelligent questions. E.g., "Implementation XXXX is in place. We do not do YYYY. The risks associated with not doing YYYY are mitigated by ZZZZ."*	*This is where the decision maker identifies whether the current state is satisfactory, acceptable, unacceptable, or unacceptable and urgently in need of attention*	*There's always notes column, so...*
Yes	*See the following descriptions at the 1.X level.*		
Yes	We use a spreadsheet instead. Bob maintains that spreadsheet in Google Drive. I know this because he told me so. - Love, Craig	2-Acceptable	An automated tool would be great to have, but we're just hoping that the university moves on this. We can't afford it. You guys are doing great with the spreadsheet. - Love, JAM

… and, then give your people some freedom to innovate and respond to your environment, your mission, and your specials.

Special Topic: Identifying Information Assets

This is a FOUNDATIONAL control!

“Information Assets”



CTSC

Project Mission & Interests

Trust in scientific results, reputation, safety

‘CIA’ Security Objectives

Confidentiality, Integrity, Availability

Controls

E.g. 2FA,network monitoring

By focusing on preventing “losses of information security,” CIA objectives sit between the fundamental reasons why we protect info assets and the controls we put in place.

The 'CIA' Triad of Security Objectives

Confidentiality Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity Guarding against improper information modification or destruction, and includes ensuring information authenticity. A loss of integrity includes the unauthorized modification or destruction of information, and the unauthorized control of an information system.

Availability Ensuring timely and reliable access to and use of assets. A loss of availability is the disruption of access to or use of an asset.

See, 44 U.S.C. 3542(b) and FIPS 199

Tips for Identifying Information Assets

1. Create and maintain solid documentation of what is actually there.
   a. Information Asset Inventory
   b. A solid basis for selecting controls, conducting RAs; an investment in continuity of the program.
2. Start with your information inventory (*vs* information systems) and capturing data flows.
3. Think in terms of types of information and information systems; get more detailed as needed.
4. Take the opportunity to get a handle on the security objectives for those assets.

1.2 Type of Information

⇒ *Enter a description of this information type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you'll list information that's part of this set.*

Asset Name	Short Description	Owner	Asset Detail
Insert a short name to unambiguously identify asset	*Describe the asset. Unless there's a referenced asset detail, this should include where it is and how it's accessed.*	*Who is responsible for this asset?*	*Where is there more information about this asset?*

Confidentiality:
Integrity:
Availability:

Yes, we've got a template for that.

Information Asset Details:

- What's included in this dataset?
- Why do we have it? Where is it coming from, and what do we use it for?
- How is this dataset stored?
  - Format
  - Location
  - Backups
- Where should this data travel?
  - Who and what systems should be able to access?
  - How will it get there?
  - How is that movement protected? (e.g., authentication, encryption)
- What, if anything, sets this data apart from other things in the type?

The process for info systems is similar:

2.2 Type of Information System

⇒ *Enter a description of this system type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you'll list information that's part of this set.*

Asset Name	Short Description	Owner	Asset Detail
Insert a short name, may be descriptive or may be the system hostname.	Describe the asset. Type of equipment, its function, etc. For hardware, include model and serial number when available.	Who is responsible for this asset?	Where is this asset documented in more detail?

Confidentiality:
Integrity:
Availability:

Details on information systems:

- Hardware specs & serials (if applicable)
- Software packages & major version numbers
- What data does this system touch?
- How does that data get in and out, and where does it go to / come from?
- What can this system control? How is that done?
- What does normal operation of this system look like? What runs on this system?
- How do we know when it's not behaving?
- What administrative systems control and document this system?

Q&A

Any success stories on identifying your assets and maintaining that up-to-date picture??
Any tricks or templates or deliverables you'd be willing to share?

Special Topic: Risk Assessments

Q: What is a risk assessment?

- Frequently listed as procedural control
- NOT the same as *risk management*
- Typical semi-quantitative risk assessment:
  - Gauges the relative magnitude of risk level posed by enumerated hazards
  - Can be focused on one asset or your whole project
  - *See, e.g.*, NIST SP 800-30 rev 1

Bottom line: The deliverable is an *input* to decisions around resource allocation

Ransomware infects the server with all the research data.

(Estimated) Impact

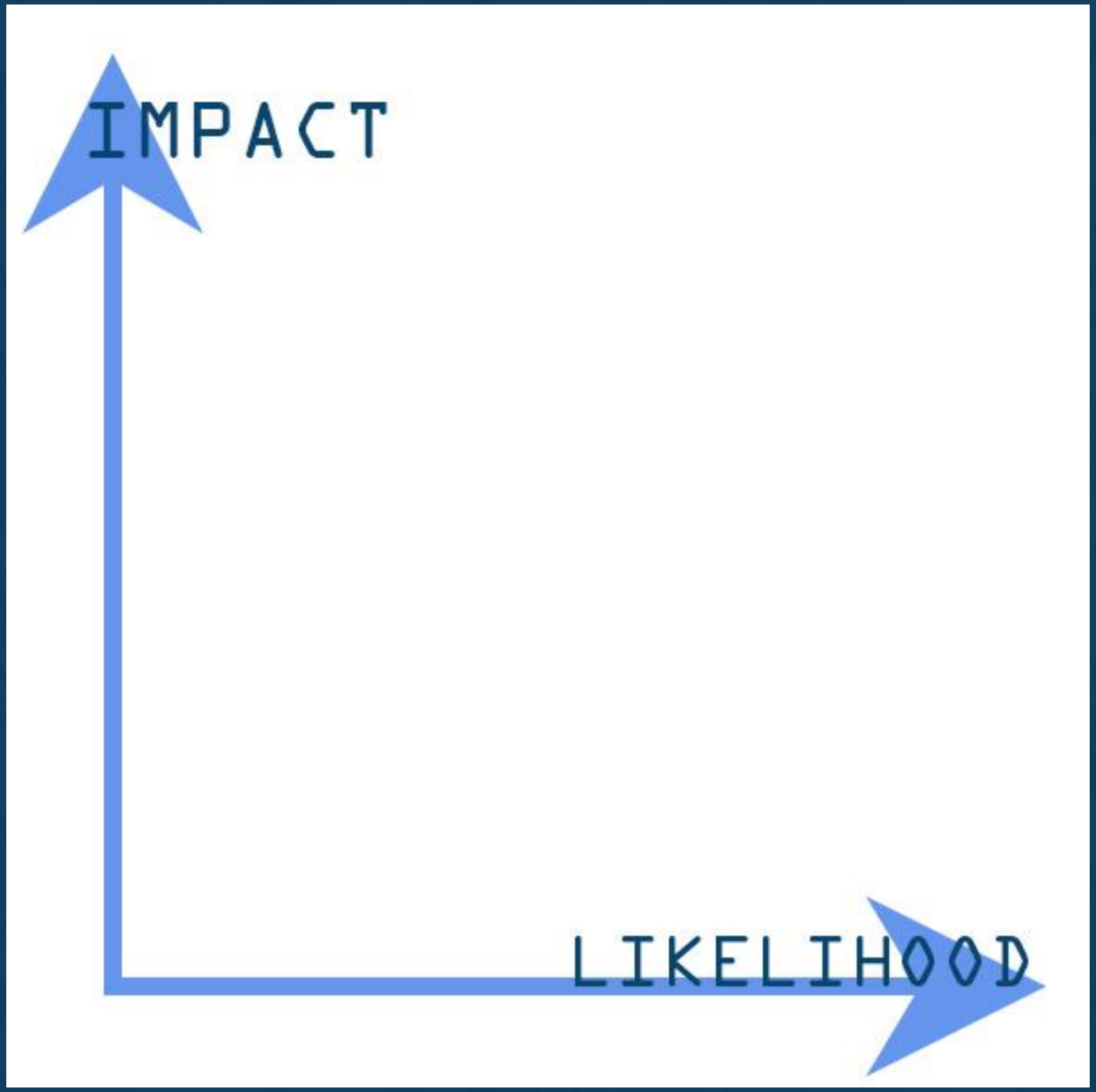
x

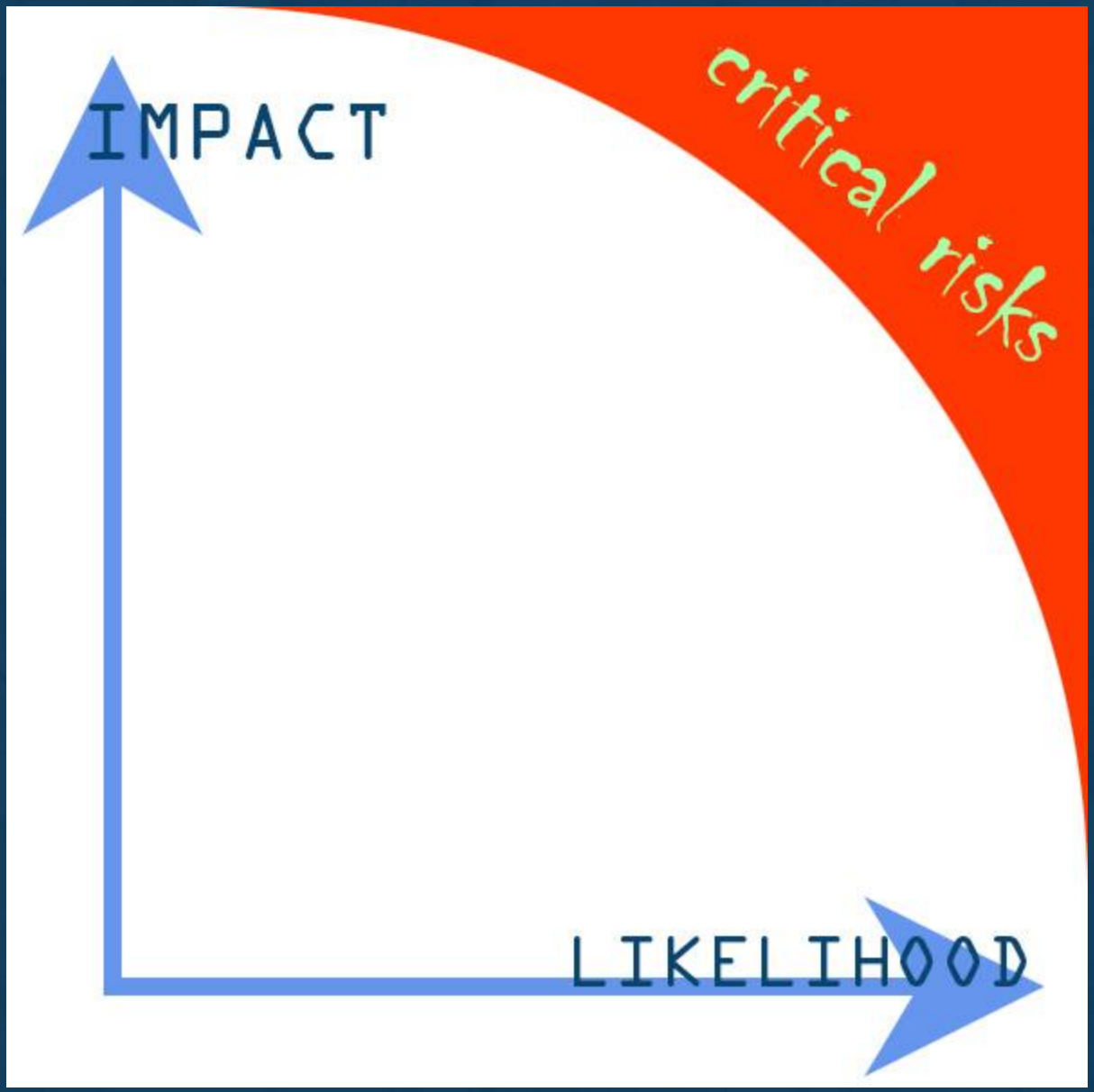
(Estimated) Likelihood

=

(Inherent) Risk (Level)

CTSC


IMPACT
LIKELIHOOD


IMPACT
critical risks
LIKELIHOOD

Benefits of a Formal Risk Assessment?

- Checks a box?
- Forcing function to account for changes in the environment (new threats, new tech, new defenses)
- Surprise findings
- Communication tool

Q: Are risk assessments the only way to allocate resources well?

A: Absolutely not.

See, again,

AFCEA The Economics of Cybersecurity

1. Focus on low-cost, high-impact interventions.
2. Prioritize defenses against common, unsophisticated attacks.
3. Utilize targeted defenses against high-sophistication, high-criticality attacks.
4. Accept risk of high-sophistication, low-criticality attacks.

Q: Are semi-quantitative risk assessments in the NIST style worth it?

A: Probably not.

Why?

1. They are expensive.
2. They generally produce invalid results particularly wrt “likelihood.”
3. They’ll most likely reinforce the fact that you are not and should be doing foundational controls.

Tips for carrying out semi-quantitative risk assessments (if you just can't help yourself)

1. Operationalize your definitions.

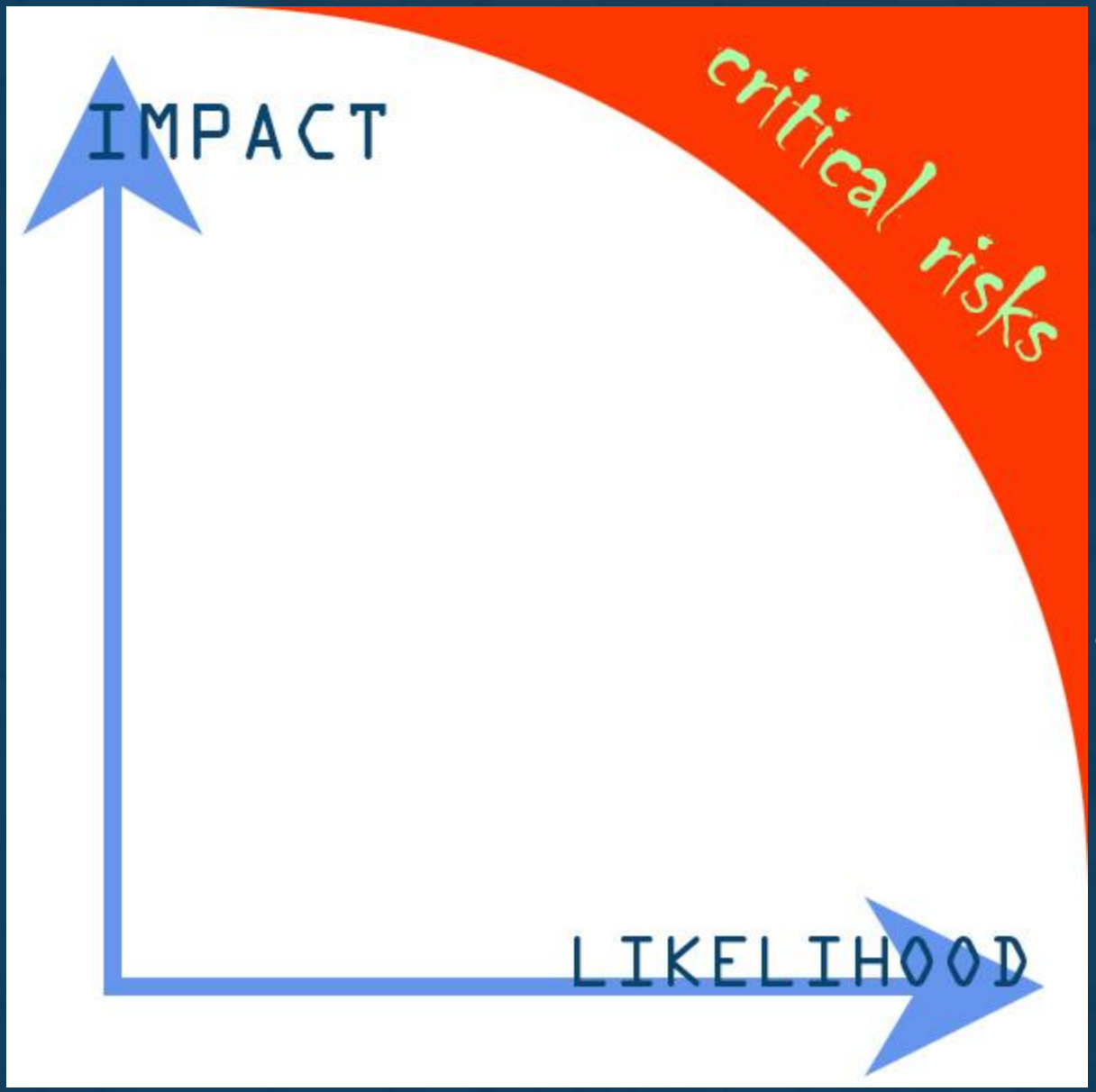
   Is "extremely likely" a frequency of every day, week, or month?

2. Consistently apply concepts from risk to risk. Don't switch definitions based on the risk!
3. Consistently characterize threats events/hazards; include a set of common elements in each description. (Or, use a catalogue; see Appendices E and F of SP 800-30)
4. Solicit estimates from multiple sources / validation.
5. We have a relatively simple table you can use. trustedci.org/guide

General Risk Assessment Recommendations

1. Consider foregoing or holding off. Get the pillars in place first.
2. Skip the expensive, invalid quasi-quantitative assessment.
3. Consider using the Open Science Cyber Risk Profile.
   https://trustedci.org/oscrp/
4. Take an asset-based approach (particularly if your project and/or cyber program are new).
5. Focus on your most critical assets and data flows.
6. Look for critical risks, particularly black swans and grey pigeons.

Black swans



CTSC

Q&A

Anyone want to share experience with risk assessments?

3.d.
Addressing Project Phase

Kickstarting a program

A couple case examples...

Case 1… a newly funded facility, in construction, kickstarting a program

1. Governance, Resources, Controls from Day 0

2. Architect, select, and build information assets and environments that are more secure and resilient from the start!

Start early and bake it in at the beginning

CTSC

Case 2… an operational facility, kickstarting a program

1. Identify Critical Risks
   a. *Grey pigeons*. High frequency incidents. Reduce frequency and aggregate impact.
   b. *Black swans*. Reduce impact / contingency planning.
2. Identify Governance and Control Gaps
   a. Roles and responsibilities. Who has the ball?
   b. Think CSC's top 4 or 6. "Cyber hygiene."
3. Implement Targeted Controls
   a. *Low-hanging fruit first* (low cost, high positive impact)
   b. Phases or waves. Can't and probably shouldn't do everything at once.
4. Identify, Protect, Detect, Respond, Recover

4.
Maintaining a program

Outline of Section 4

- Are Policies and Controls enough?
- Communicating the Program
  - Getting buy-in
  - Training
- Continuous Monitoring
- Incident Response
- External Resources

Now that we have policies and controls in place, are we done?


GATE

CTSC


AUTHORIZED
PERSONNEL
ONLY


AUTHORIZED
PERSONNEL
ONLY
GATE

Who cares about your cybersecurity program?

- ...and what do I do with everybody else?
- Approaches to generating buy-in
  - Top-down: funding agency requirements, specter of consequences
  - Bottom up: CYA, okay to be territorial
  - Theoretically, everyone is in favor of security (so long as it doesn't get in their way)
  - Partnership: they don't want to fail; you're there to help them succeed

Beware of Shadow IT

Shadow IT - What is it?

- Projects conducted out of compliance with policies and without oversight from central IT
  - Use of cloud for computational or data storage services outside of support structure
  - Includes “critical server” located under Joe’s desk
  - Tradeoff with rapid, agile development
  - Surprise turnover to central IT on deployment
- Understand who the renegades are and work with them

Inside Users / Personnel:

- “Cyber Hygiene”

  “It is the online analogue of personal hygiene, and encapsulates the daily routines, occasional checks and general behaviours required to maintain a user's online "health" (security)” - Wikipedia

- Specific policies that impact their job
- When and where to get help or ask a question

Outside Users:

- AUP (Acceptable Use Policy)

Training methods matter.

Providing information is only half the job.

Training:

- In person
- Be personable
- Make it relevant
- Sales, not just exposition

The everyday experience will teach your team more than any training you give them.

What is it teaching them?

Continuous Monitoring

i.e., Appropriately Frequent Monitoring

- Threat monitoring
  - SANS Internet Storm Center https://isc.sans.org/ ; US-CERT; Twitter: @USCERT_gov and @SANSInstitute; CI Vulnerabilities cv-announce@trustedci.org
- Configuration and Vulnerability Management
  - OS and application software checked that current, patched versions are installed and securely configured
- Log collection and analysis
  - Logs from devices provide data about attacks
  - Many management tools are available; also external monitoring services

Incident Response

- Develop and communicate a plan of action
  - For compromised desktop, server, network
- Include a communication plan
  - Who talks to management, media, CERT, etc.
  - What frequency and kind of information passed on
- Post-mortem analysis and report
  - Root cause analysis
  - Gauge effectiveness of controls
  - Develop remediation plan, if necessary

RULE: Don't talk to the media

Incident Response Plans

- A determined attacker will succeed and there are many places to hide
- If you are on the Internet, then you are compromised -- the problem is to find them and recover to a “good place”
- Create a general plan based on “PDCA” or “OODA” loops (see Wikipedia articles for explanation)

Douglas Adams, HHGTTG

CTSC

External Resources and Partners

- Your Internet Service Provider
- Parent Institution
- Peer Organizations
- Commercial Security Consultants
- REN-ISAC
- Bro Center of Expertise
- FBI Cyber Crime Unit
- CTSC

Using External Security Sources

- NIST SP 800-35 & SP 800-36 have advice (2003)
- Get insight into what external sources have to offer
  - Balance risks, costs, and benefits
  - Trade-offs: control, resource demands, available expertise
- Clarify expectations
  - Ensure contract service level agreement (SLA), memorandum of understanding (MOU), or other agreement outlines relevant security expectations

Q&A

5.
Evaluating and optimizing a program

Reminder:
Phase Matters

What are we evaluating?

How do you measure cyber wellness?

Health	How functional are we? How sick?
Maturity	Do we have the right policies, procedures, processes, and resources in place?
Susceptibility	Can we keep malicious actors at bay?
Resilience	Will we bounce back when things go wrong?
Compliance	Are we doing everything someone else told us to do?
Growth	Did we make improvements over time?

A note about existing cybersecurity maturity models

1. Tend to be very policy focused. You can be "mature" and still sick as a dog.
2. Tend to leverage very little (if any) outcome measurement.
3. Can be difficult or costly to operationalize.
4. Old favorite (Booz Allen) is gone. Pay wall.
5. Maturity alone (just like compliance alone) will *never* give you a complete picture of your health and wellbeing.

Third Party Evaluations

1. Types:
   a. "Blue team": Breadth, Cooperative, Programmatic
      i. Tough love: Can be more or less friendly / trusting
      ii. CTSC engagements
   b. "Red team": Depth, Adversarial (e.g., pen-testing)
2. Focus / standard varies: mission assurance vs. audit against a particular standard / control set vs. identifying threat vectors vs. owning you and explaining how
3. Deliverables vary: prioritized recommendations vs. unprioritized recommendations vs. noncompliance

Self Evaluations

1. Blueish:
   a. Project based: Did we meet the objectives in our plan?
   b. Standards based: How do we compare to the archetype?
   c. Benchmark based: How do we compare to our peers?
2. Redish:
   a. Table top exercises
   b. Simulated incidents
   c. Real incidents: How did we do during a real incident? What can we improve?

The Positives Matter

1) Security is about surviving and thriving.

2) Celebrate both.

6. Conclusion

Next steps for the NSF CCoE wrt cybersecurity programs

1. Develop Guide v2
2. Assist LFO w/ Large Facilities Manual section on cybersecurity
3. Facilitate Large Facilities Security Team
4. Promote participation in 2017 NSF Community Cybersecurity Benchmarking Survey

References

CTSC's Community Resources (Email Lists, Guide, IAM, SwA, OSCRP, Vulns)

https://trustedci.org/ (expand left Community Resources nav)

AFCEA: The Economics of Cybersecurity

https://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf (8 pgs)

CIS Critical Security Controls

Poster: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf (1 pg)

Full document: https://learn.cisecurity.org/20-controls-download (requires registration) (96 pgs)

Back to Basics
https://www.sans.org/reading-room/whitepapers/analyst/basics-focus-first-cis-critical-security-controls-37537 (5 pgs)

Australian Signals Directorate: Essential Eight

https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf (2 pgs)

https://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf (top 4) (42 pgs)

California Data Breach Report, 2016

https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (focus on the Executive Summary and Recommendations) (5 pgs)

Acknowledgements & Thanks

- National Science Foundation
- Bret Goodrich & DKIST / NSO
- Contributors & Commenters, esp. Susan Sons and Von Welch
- You!

This document/presentation is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grant ACI-1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

CTSC

Thanks!

CTSC